Documento in consultazione - Provvedimento del 29 aprile 2021
Disposizioni in materia di sorveglianza sui sistemi di pagamento e sulle infrastrutture strumentali tecnologiche o di rete –

Riferimento	Commento	
1 - Generale - allineamento a normative internazionali	In aggiunta agli standard di supervisione internazionali – tra cui i Principles for Financial Market Instrastructures PFMIs - è ragionevole presumere che il quadro di sorveglianza sui sistemi di pagamento e sulle infrastrutture strumentali tecnologiche o di rete della Banca d'Italia andrà a coordinarsi anche con i principi informatori, gli obiettivi e le disposizioni del Digital Finance package. Tale package contiene le proposte di regolamento europeo in materia di • resilienza operativa digitale e cyber sicurezza - come disciplinata dalla proposta di regolamento europeo DORA (COM/2020/595 final) e dalla proposta di direttiva collegata che armonizza il quadro normativo (COM/2020/596 final); • mercati delle cripto-attività ed emittenti di token di moneta elettronica significativi - come disciplinati dalla proposta di regolamento europeo MICA (COM/2020/593 final); • regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito DLT , per garantire una crescente convergenza e armonizzazione del sistema di vigilanza (COM/2020/594 final). Laddove dovesse emergere la necessità di integrare la disciplina prevista dalle "Disposizioni" a seguito dell'evoluzione tecnologica o per la diversificazione dei modelli di servizi, **potrebbe essere utile in momenti successivi prevedere la possibilità di adottare norme tecniche di regolamentazione aggiuntive da allegare alle "Disposizioni" stesse**.	
2 - Generale – ambito di applicazione	Di rilievo la estensione delle Disposizioni dai sistemi di pagamento alle infrastrutture strumentali tecnologiche e di rete e l'ampiamento dell'ambito di applicazione anche a "fornitori di servizi tecnici" in **aderenza al principio "same services/activities, same risks, same rules and same supervision**", e, naturalmente, al principio di proporzionalità. Al fine di garantire una sempre maggiore affidabilità ed efficienza del settore dei pagamenti, si rappresenta **l'importanza di individuare con chiarezza i soggetti (soggetti tradizionali e new-comers) che svolgono funzioni ed erogano servizi critici** compresi quelli esternalizzati o appaltati a fornitori terzi affinché adottino modalità idonee a presidiare i rischi sistemici - operativi e di sicurezza - che possono influire sul settore dei pagamenti nazionale ..	
3 - Generale – guida operativa ai controlli	Il Provvedimento del 2012 è accompagnato da una apposita "guida ai controlli". Tale guida contiene informazioni esplicative del Provvedimento e riporta in allegato anche un "percorso di analisi" utile agli operatori per condurre esercizi di autovalutazione per la piena rispondenza alle disposizioni stesse. Al riguardo si suggerisce di **aggiornare il percorso di analisi / Key questions**.	
4 - Generale – traduzione del testo anche in inglese a soli fini informativi	Una volta consolidato il testo si suggerisce – se possibile - di **distribuire agli operatori destinatari della normativa anche una versione in inglese del testo ai soli fini informativi**. Questo per facilitare in contesti europei e internazionali maggiore precisione nella terminologia e nel glossario e nei requisiti.	

Riferimento	Commento	
5 - Glossario – “sistema dei pagamenti” e “sistema di pagamento”	Nel glossario e nelle definizioni compare una distinzione tra “sistema **dei** pagamenti” e “sistema **di** pagamento” chiara e precisa. E’ però possibile che in lettori non attenti si possano generare dubbi e incertezze sui termini. Valutare se dare più evidenza alla sostanziale differenza dei termini in glossario introducendo ad es. – in luogo di “sistema” dei pagamenti – un termine diverso quale “schema dei pagamenti” oppure “eco-sistema dei pagamenti”.	
6 - Glossario – sequenza delle definizioni	Leggendo le definizioni a glossario in sequenza – • i termini a), b) c), d), e) sono specifici dei sistemi di pagamento • i termini f), g), h) riguardano connotati di sicurezza dei sistemi • i termini i), j), k), l) riguardano ruolo previsti nei sistemi di pagamento • i termini m), n), o) riguardano attività nei sistemi di pagamento • il termine p) un ruolo specifico • il termine q) una attività nei sistemi di pagamento • il termine r) un connotato di funzionalità operativa dei sistemi • i termini s) e t) altri ruoli e funzioni Da **valutare se opportuna una diversa sequenza dei termini**. Ad es • i termini a), b) c), d), e) in quanto sono specifici dei sistemi di pagamento • i termini m), n), o) in quanto riguardano attività nei sistemi di pagamento • il termine q) in quanto attiene a una attività nei sistemi di pagamento • i termini f), g), h) in quanto riguardano connotati di sicurezza dei sistemi • il termine r) quale connotato di funzionalità operativa dei sistemi • i termini i), j), k), l) in quanto riferiti a ruolo previsti nei sistemi di pagamento • il termine p) ruolo specifico • i termini s) e t) altri ruoli e funzioni	q
7 - Art 6 - Esternalizzazione – criteri per individuare i fornitori	L’attuale formulazione del secondo paragrafo elenca una serie di criteri da seguire per individuare i fornitori tra cui <<< iii) le procedure utilizzate per rilevare, reagire e recuperare informazioni da incidenti di sicurezza informatica >>>. Si concorda con la necessità di portare la massima attenzione ai temi cyber. Da valutare se opportuno **ricordare in tale contesto anche le procedure per gestire i malfunzionamenti, gli incidenti operativi e ICT.** Fosse ritenuto opportuno, si potrebbe formulare il punto nel seguente modo: <<< iii) le procedure utilizzate per rilevare, reagire e recuperare informazioni **da malfunzionamenti** e da incidenti di sicurezza informatica >>>.	

Riferimento	Commento	
8 - Art 6 - Esternalizzazione – criteri per individuare i fornitori	Con riferimento al criterio <<< v) gli assetti organizzativi adottati per l'identificazione e la gestione dei rischi e le relative linee di responsabilità >>> - fosse ritenuto opportuno - valutare se **elencare tra i criteri anche i sistemi di controllo interno** che un operatore deve porre in essere per presidiare i rischi potenziali. con una formulazione della frase tipo criterio <<< v) gli assetti organizzativi adottati per l'identificazione e **la gestione dei controlli**, dei rischi e le relative linee di responsabilità >>>.	
9 - Art 6 - Esternalizzazione	L'articolo pone la dovuta attenzione ai temi di sicurezza e IT (secondo paragrafo) e al contratto nel caso di servizi esternalizzati. Da valutare in questo contesto oppure in un ambito più specifico (es. guida operativa dei controlli) se **porre anche attenzione alla esternalizzazione dello sviluppo di parti di software** e alle conseguenti attività di controllo qualità, accettazione, testing e integrazione con altri moduli o componenti software.	
10 - Art 13 – obblighi informativi – l) regole di funzionamento del sistema	In aggiunta alle regole di funzionamento del sistema potrebbe essere utile all'Autorità **acquisire le definizioni dei termini che il gestore del servizio utilizza per identificare i propri servizi** e le relative infrastrutture applicative, tecnologiche e di connettività. Questo per perimetrare il contesto operativo, organizzativo, e tecnologico di erogazione dei servizi oggetto del Provvedimento, per facilitare la comprensione della documentazione interna all'azienda e per identificare gli asset utilizzati per erogare i servizi.	
11 - Art 19 – fornitori di servizi tecnici – identificazione	Primo paragrafo al punto c si introduce il termine di "**dati sensibili di pagamento**". Tale termine non compare in glossario e in altri passaggi della proposta di Provvedimento. Può essere interpretato in modo discrezionale o riferito ad altri standard (es. PCI-DSS)	
12 - Art 19 – fornitori di servizi tecnici – identificazione	L'articolo esclude da obblighi di cui al comma 1 i fornitori di servizi non specificamente funzionali all'erogazione di sevizi o funzionalità di pagamento tra i quali: fornitori di energia, luce, gas, acqua, fornitori di sevizi offerti infragruppo. **Nell'elenco non si citano i fornitori di servizi di telecomunicazioni e i servizi di infrastrutture, di facilities e di location di data-centre**. Si ritiene pertanto che tali categorie di fornitori rientrino negli obblighi.	
13 - Art 19 – fornitori di servizi tecnici – obblighi di notifica inizio e fine attività	A migliore precisazione dell'esclusione – se ben interpretato il testo - si suggerisce una possibile riformulazione del testo DA <<< … sono esclusi dall'obbligo di cui al comma 1 ….. >>> A <<< Sono esclusi dall'obbligo **di notifica** di cui al comma 1 ….>>>	
14 - Art 20 – titolo dell'articolo (ambito applicativo)	Tale articolo 20 è citato anche nella definizione dei fornitori di servizi critici (capoverso "l" – elle). L'articolo indica le modalità con cui i fornitori critici sono individuati e i criteri considerati prioritari per la loro individuazione. Valutare se riformulare il titolo dell'articolo: DA <<< Ambito applicativo>>> A <<< Fornitori critici>> oppure <<< Individuazione dei fornitori critici >>>	

15 - Art 22 – obblighi informativi	Come per i gestori dei sistemi di pagamento, **anche per i fornitori di servizi tecnici potrebbe essere utile acquisire le definizioni dei termini che il gestore del servizio utilizza** per identificare i propri servizi e le relative infrastrutture applicative, tecnologiche e di connettività. Questo per perimetrare il contesto operativo, organizzativo, e tecnologico di erogazione dei servizi oggetto del Provvedimento, per facilitare la comprensione della documentazione interna all'azienda e per identificare chiaramente gli asset utilizzati per erogare i servizi	
16 - Art 22 – obblighi informativi	Nel leggere i punti elenco **non compare la richiesta di documentazione utile a comprendere il funzionamento del servizio erogato** ed eventuali standard contrattuali e livelli di servizio.	
17 - art. 19 – attestazione Regolamento EU e norme tecniche di regolamentazione	Si chiede di comprendere se **l'attestazione richieda degli esercizi preliminari di autovalutazione** da parte dei soggetti destinatari della norma, oppure azioni di sorveglianza da parte del regolatore.	
18 – art 20 – servizi tecnici essenziali	Al secondo capoverso dell'articolo si introduce il termine di "**servizio tecnico essenziale**". Tale termine non compare tra le definizioni e in altri passaggi della proposta di Provvedimento.	
19 – art 21 – fornitori critici di servizi tecnici	Primo paragrafo – considerare che i servizi potrebbero essere offerti - oltre che su base contrattuale - **anche con certificazione** facendo riferimento ai servizi oggetto di certificazioni / omologazioni SITRAD	
20 – art 21 – fornitori critici di servizi tecnici	All'ultimo capoverso dell'articolo si fa riferimento a "**fornitori critici di servizi tecnici**". Salvo errori di lettura, tra le definizioni e in altre parti del documento si fa riferimento a "fornitori di servizi critici".	
21 - art. 22 – obblighi informativi	Alla lettera d) si chiedono indicazioni di piano strategico e operativo per gli aspetti concernenti i **servizi "critici" offerti**. Valutare se opportuno chiedere indicazioni sui servizi offerti e rientranti nel perimetro, senza limitarsi ai servizi ritenuti "critici".	
22 - art. 22 – obblighi informativi	Tale articolo si applica ai fornitori di servizi tecnici. Potrebbero essere di interesse anche **informazioni relative all'organizzazione dei controlli interni** oltre che sul presidio dei rischi.	
23 - art. 22 – obblighi informativi	Tale articolo si applica ai fornitori di servizi tecnici. Potrebbero essere di interesse anche **informazioni relative alle esternalizzazioni in essere** – se presenti (es. elenco dei sub-fornitori)	
24 - Possibile pluralità di ruoli in capo allo stesso operatore e conseguenze su adempimenti informativi	Se un gestore di sistema di pagamento al dettaglio svolge anche ruoli come fornitore di servizi tecnici potrebbe essere soggetto – in base al servizio - agli obblighi informativi dell'art. 13 e anche a quelli dell' art. 22. Si suggerisce di prestare attenzione a tale eventuali casistica nelle comunicazioni ai gestori/ fornitori.	